BeyondTrust

AD Bridge
Best Practices Guide

TC:2/28/2024

Table of Contents

AD Bridge Best Practices Guide

Why use best practices with AD Bridge (ADB)? Best practices ensure the optimal setup and performance with your ADB product. The current best practices have been shown to be the most efficient way to work.

AD Bridge allows management of Linux and Unix systems within Microsoft Active Directory. AD Bridge includes support for AD Bridge Cell Technology, two-factor authentication, Group Policy, and reporting features.

Enterprise Tools

Because both workstation and server operating systems are supported, it is important to note that this software should be installed on a *management workstation*, and not on a *domain controller*. The appropriate installer should be used on each platform. The installer name denotes the version. This management workstation can be a *terminal server*, a *user's desktop*, or a *shared desktop*.

AD Bridge software authentication architecture installs no services that need to be run on a Windows server. Because of this, administrators can keep domain controller installations clean of non-Microsoft software, and they can perform maintenance on these servers with no special considerations for AD Bridge client computers.

> *Group Policy administration should be handled for AD Bridge in the same manner as suggested by Microsoft. For more information, see Best Practices for Securing Active Directory, at https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory.*

Naming Conventions

Why have and follow naming conventions? To keep your work and data *organized* and to bring *consistency*, which makes it easy to process and get results. Before taking any actions with naming conventions, review these best practices carefully. We recommend following the naming practices outlined in the following links.

Systemd User and Group Naming Syntax

https://systemd.io/USER_NAMES/

Active Directory User and Group Naming Requirements

https://social.technet.microsoft.com/wiki/contents/articles/11216.active-directory-requirements-for-creating-objects.aspx

Configurable Characters

Configurable characters are used in specific ADB designations. While these are configurable, we recommend using the default values.

- **DomainSeparator**: Character used to designate the domain name separator.
- **SpaceReplacement**: Character used to designate space characters in the name of an object.

> ***Note:*** *The* ***DomainSeparator*** *and* ***SpaceReplacement*** *characters should never overlap characters used in any of the following: LDAP CN, distinguishedName, SamAccountName, UPN, uid, displayName.*

> *For more information about configurable characters usage in ADB, see Lsass, at https://www.beyondtrust.com/docs/ad-bridge/how-to/configuration-tool/lsaas.htm.*

Active Directory Best Practices

Before taking any actions with Active Directory, review these best practices carefully.

AD Bridge Cells provide a means of directly managing Unix identities in Active Directory. *Best practices are to use Cells rather than Unprovisioned mode wherever possible.*

This is so a user's Unix group membership can be limited to less than 16 groups when required for NFS (or 32 groups for Solaris) without impacting normal Windows group membership management practices.

Directory Integrated Mode

After installing the AD Bridge tools, the first determination that must be made regards *Directory Integrated* or *ID Range*. *Directory Integrated Mode is strongly preferred*.

This causes all lookups to use indexed attributes in AD, lowering the cost of each lookup against the AD domain controller (DC). Windows 2012 Forest Mode forests with Windows 2012 R2 domain controllers can be transitioned to Directory Integrated Mode without extending the AD Schema. Because Microsoft forest modes are moving in this direction, and because of performance increases, Schemaless Mode should be avoided where possible.

Cell Design

AD Bridge Cells allows managing overlapping Unix identities within a single Active Directory organization for AD Bridge. Cells work in Directory Integrated or Schemaless Mode, as described above. There are two possible cell structures:

- **Named Cells:** Named Cells store Unix identity information (**uid**, **uidNumber**, **gidNumber**, **gecos**, **unixHomeDirectory**, **logonShell**) in a subcontainer of whichever Organizational Unit (OU) is associated with the cell. Whether a user exists in the local domain or a trusted domain, the Unix identity information exists in an object in the cell. In other words, a Named Cell may reference users or groups from outside the current AD domain, but stores data in the domain where the computer is joined.
- **Default Cell:** In contrast to Named Cells, there is a single Default Cell, and it is *enterprise wide*. That is to say, all trusted Microsoft Active Directory Global Catalogs are part of the single Default Cell. However, individual AD Domains opt-in to the Default Cell by creating the Default Cell object in the *root* of those domains. In the Default Cell, the Unix identity information is stored in the same OU as the user object that the Unix Identity information is related to. This enforces a single Unix identity for a single AD user across the entire enterprise. Therefore, the Default Cell should be viewed as the ultimate authority for Unix information within an enterprise.

Cells store Unix identity information separate from other cells. This allows a single user or group to have different names, or different numerical ID values (UID or GID) in different environments, all tied back to the same AD identity. This also allows multiple users or groups to have *overlapping names* or *numerical ID values* (UID or GID) in separate environments. Each cell will require additional overhead for Standard Operating Procedure for account management and for troubleshooting end-user log in issues, as both cases will require the additional step of determining which cell the operation must be performed against.

> ***Note:*** *To keep end-user and help desk troubleshooting complexity to a minimum, while allowing the flexibility of cells, BeyondTrust suggests no more than four cells.*

Cells are only a method of managing conflicting Unix identities within an environment. While they can technically be used to limit end-user access to a system, this is against the design of AD, which allows all users to be *seen* by any joined client, but limits authorization based on other methods. Therefore, BeyondTrust suggests strongly that cells not be used as access control (authorization), but only as a part of the authentication system, and that the AD Bridge setting **RequireMembershipOf** or **Allow Logon Rights** be used for authorization.

Directory Integrated Mode Cells

In Directory Integrated Mode, the Default Cell stores the Unix identity information directly on the user or group object, in the exact same manner that **First Name** (**givenName**), **Address** (**address**, **city**, **state**), and **Email** (**emailAddress**) attributes are.

In Directory Integrated Mode, Named Cells create objects of class **PosixAccount** and **serviceConnectionPoint** which are linked back to the user or group object associated with the cell object.

Because the Directory Integrated Mode Default Cell stores the information directly on the user or group object, existing Identity Management (IDM) products do not need to be modified to provision users for the Default Cell in Directory Integrated Mode. This also allows non-AD Bridge systems which use the RFC2307 attributes to use the same identity information as AD Bridge.

Default Cell Directory Integrated Mode is therefore the preferred method for all AD Bridge installations. In all cases where Unix identity information can be made to be non-overlapping, the Directory Integrated Mode Default Cell should be used.

Directory Integrated Mode Named Cells are recommended wherever multiple cells beyond the Default Cell are required.

Schemaless Mode

IMPORTANT!

*Schemaless mode is **deprecated**. The content below is for information only.*

Because of the performance benefits of Directory Integrated Mode Cells, and that Microsoft AD is moving towards Directory Integrated Mode by default, Schemaless Mode is *deprecated*, but 100% supported. The AD Bridge clients determine cell and schema configuration upon every startup. This allows migration from *Schemaless Named Cells* to *Directory Integrated Named Cells* to be as simple as dragging a computer object between OUs.

However, because of how the data is stored, migration from a Non-Schema Default Cell to a Directory Integrated Mode Default Cell configuration requires more work, more steps, and more potential risks than any other cell migration.

For migration and long-term support purposes, Schemaless Mode cells should only be created as Named Cells.

User Rights

Because AD Bridge software joins the Unix computers to AD with the same API calls as Microsoft Windows uses, in most cases, the same rights are required in AD for Unix administrators as Windows administrators need to join the domain. BeyondTrust recommends that Unix computer accounts be either pre-staged or that the Unix administrators be delegated control to an OU that all Unix computers will be joined to.

For more information on pre-creating computer accounts, see Microsoft's documentation at https://support.microsoft.com.

Do Not Provision the Domain Users Group

By default, the Domain Users group is provisioned to new cells so there is a GID for new users. This is to streamline deployment but is not recommended for production use.

In environments with frequent user or group enumeration, this will generate a lot of LDAP traffic to list all the provisioned users and groups. By default, all users are part of Domain Users and this will cause enumeration of all users in the domain.

We recommend creating a group for the cell to limit the enumeration.

Netlogon Authentication

IMPORTANT!

This is an early release feature. We recommend enabling the feature in a test environment and sending in feedback.

We recommend enabling Netlogon authentication to validate the domain controller (DC) through a secure channel connection. This adds an extra level of security when communicating with the domain.

Enable Netlogon authentication using the following command:

```
/opt/pbis/bin/config DCValidationSupport true
```

DCValidationSupport

```
/opt/pbis/bin/config --verbose DCValidationSupport
Current local policy value: false
Using default value: false
Executing command: /opt/pbis/bin/lwsm refresh lsass
Refreshing service: lsass
```

DCCacheExpiryInterval

DCCacheExpiryInterval is the length of time the agent holds onto the cached DC information.

```
/opt/pbis/bin/config --verbose DCCacheExpiryInterval
Current local policy value(s): 1440
Using default value(s): 1440m
Executing command: /opt/pbis/bin/lwsm refresh lsass
Refreshing service: lsass
```

DCCacheEnabled

The **DCCacheEnabled** allows the agent to cache the DC information.

```
/opt/pbis/bin/config --verbose DCCacheEnabled
Current local policy value(s): true
Using default value(s): true
Executing command: /opt/pbis/bin/lwsm refresh lsass
Refreshing service: lsass
```

Active Directory Best Practices Summary

- Use Cells.
- Use Directory Integrated Mode.
- Use **Allow Logon Rights** or **RequireMembershipOf** for access control.
- Use the Default Cell in Directory Integrated Mode where possible.
- If Schemaless Mode is required, use only Named Cells.
- Delegate Control to Unix Administrators to join AD Bridge computers.
- Do not provision the Domain Users group.

AD Bridge Reporting Tool Best Practices

Before taking any actions with the AD Bridge Reporting Tool, review these best practices carefully.

Database

AD Bridge Reporting requires an SQL Server database. Because SQL Server integrates fully with AD, database ownership and rights can be set directly for AD users, and SQL Server supports Integrated Security (which does not require username and password combinations in connection strings).

Collector Servers

AD Bridge Reporting also requires Windows platforms to run the Collector server and Enterprise Database Forwarder. These are the only Windows services that AD Bridge software ships. Best practice for network design and WAN traffic management is to place the Collector servers closer to the AD Bridge agents.

To support auditing in case of a Collector failure, the AD Bridge agents only need to be pointed to a different collector. To support this situation, we suggest that the customer build a number of Collector servers equal to or greater than the following formula:

Total Collectors = ((number of AD Bridge Agents) / 400) + 1

Group Policy

To use the full functionality of the reporting solution, BeyondTrust suggests setting all of the **Enable AD Bridge Auditing** settings in Group Policy, and enabling the **Syslog Auditing** policy.

Reporting Tool Best Practices Summary

- Use MS SQL Server.
- For network design and WAN traffic management, place the Collector servers closer to the AD Bridge agents.
- Use one collector for each 400 AD Bridge Agents.
- Use Group Policy to enforce AD Bridge Reporting Settings.

Group Policy Best Practices for AD Bridge

Before taking any actions with AD Bridge Group Policies, review these best practices carefully.

Object Linking and Delegation

BeyondTrust recommends the same best practices for Group Policy Objects as Microsoft recommends.

> *For more information, see best practices from Microsoft Group Policy MVP Darren Mar-elia at https://www.itprotoday.com/group-policy/group-policy-design-best-practices.*

AD Bridge has an available Target Platform Filter to limit Group Policy to apply only to certain operating system types. This filter's use should be minimized in the same way as any other filter listed in the *Group Policy Design Best Practices* article.

Settings

The Configuration **wizard** in the installation directory provides the initial best practices for all customers' AD Bridge settings. Those settings not enforced in this initial Group Policy Object have been optimized on the client by the BeyondTrust team for each version of AD Bridge. Some settings, however, are optimized for general use. These settings should be updated for different system times, as listed below.

General Recommended Policies

- **AD Bridge Settings:**
  - Authorization:
    - Enable use of the Event Log
    - Disable user credential refreshing
- **Group Policy:**
  - Enable use of the Event Log
- **Event Log:**
  - Keep a 90+ day history in the Event Log
  - Set a maximum disk size at 120MB
  - Remove events as needed
- **Logging and Audit Settings:**
  - Enable AD Bridge Auditing in the **Syslog** settings

Systems Not Using User Policies

- **Group Policy:**
  - Disable user logon Group Policy setting processing

Servers

- **AD Bridge Settings:**
  - Logon
    - Disable creation of home directory - if using NFS mounted home directories
    - Disable creation of **k5login** - if using NFS mounted home directories
- **Event Log:**
  - Keep a 90+ day history in the Event Log
  - Set a maximum disk size at 120MB
  - Remove events as needed

Workstations or Laptops

- **AD Bridge Settings:**
  - Logon
    - Enable creation of home directory - except when using NFS mounted home directories
    - Enable creation of **k5login** - except when using NFS mounted home directories
- **Event Log:**
  - Keep a 60+ day history in the Event Log
  - Set a maximum disk size at 75MB
  - Remove events as needed

Group Policy Creation

Many AD Bridge Policy settings control specific Unix files in their entirety. The sudoers and Automount policies are two examples.

In all cases when these polices are to be used, we strongly recommend that the files be created and tested on a Unix system, then transferred directly into Group Policy, by using the **gp-admin** tool from a Linux station, or binary transfer to a Windows computer to upload with Group Policy Management Console (GPMC).

Best practices would be to never modify these settings on a Windows computer directly.

Password Prompts

We do not recommend using the Password Prompts policy. If Password Prompts are in use, the expected account type is displayed. For example, Active Directory or Local Account. This policy setting may encourage brute force attacks.

Allow Logon Rights

Allow Logon rights groups should not be enabled in a cell. It is evaluated by **lsass** as a list of security identifiers (SIDs) to match against the SIDs provided in the Privilege Account Certificate (PAC) of the Kerberos ticket. Evaluation beyond the level of the SID is not required, and as such, groups don't need to be provisioned. Provisioning groups provides additional information to non-privileged users as to who

can log into the Unix host.

Additionally, if AD Bridge is unable to determine authoritatively all groups the user is in, access is denied. This can occur if there are DENY access control lists (ACLs) in place. NFSv4 has DENY ACL functionality, so this can also apply to Unix systems.

Delegate either **Domain Computers** or to a **Linux Computers** group so the computers can see the information required to do the lookups.

Group Policy Best Practices Summary

- Use OU design and linking, as a preference to filtering.
- Use different settings for servers and workstations.
- Use the Unix **gp-admin** tool to manage Unix files.

Unix Best Practices for AD Bridge

Before taking any actions with Unix for AD Bridge, review these best practices carefully.

All AD Bridge Supported Operating Systems

Any time SSH is upgraded, **domainjoin-cli configure --enable ssh** should be run to verify the **sshd_config** file is set up properly to talk to AD Bridge.

After any major system upgrade (kernel patch, OS upgrade, or similar) is performed, a full rejoin to the domain should be performed. This will verify that all OS-specific files are configured properly, resynchronize any changes to the Kerberos configuration, and will also update the **operatingSystemVersion** and **operatingSystemServicePack** values in Active Directory, so that the AD Bridge Reporting (or other reporting) system can accurately reflect the environment.

BeyondTrust suggests all vendor patches be applied per the vendor schedule.

Operating System Specific

Best practices for AIX, Linux, and Solaris operating systems.

AIX

BeyondTrust recommends that PAM support be enabled and tested with all client applications prior to installing AD Bridge. While LAM is supported, PAM authentication provides standardized authentication across all environments, including AIX.

BeyondTrust recommends deprecating the practice of using the **suroot** group in favor of PAM-enabled sudo for all end-users and application owners on the AIX environment, due to difficulties managing the **suroot** group for AD users once AD Bridge is installed.

Linux

Best practices for Debian and Red Hat Linux variants.

Debian Linux Variants

No special recommendations.

Red Hat Enterprise Linux Variants

In RPM-based systems, each package owns its own PAM file, which is written, then updated by the **authconfig** process. Therefore, whenever **authconfig**, **yum upgrade** or similar command is run, customer should run **domainjoin-cli configure --enable pam** to ensure the **pam_lsass.so** entries are added back into the proper places in the PAM configuration. In some environments, customers schedule a background update from RHN on systems. After this background update is complete, **domainjoin-cli configure --enable pam** should also be run.

Solaris

We recommend Solaris 11.4 or higher. Large Solaris environments should take care to enable only the AD groups required for Unix file and sudo access.

Solaris Full Root Zones

We recommend installing AD Bridge on Solaris Zones individually. This gives the Unix administrator the flexibility to upgrade zones individually, separate from the upgrade state of the global zone. Additionally, since the join state is managed on a per-zone basis, the entire AD Bridge software installation can be managed together, on each individual zone.

Solaris Sparse Root Zones

Solaris Sparse Root zones should be managed with a *whole system* philosophy. Because certain files are only created in the global zone, when they are upgraded, all child zones should be upgraded at the same time as well. This is handled by the AD Bridge installer automatically. The join state is still managed individually on each child zone. In cases where all the zones cannot be upgraded simultaneously, the non-upgradable systems must be migrated to a new host.

Unix Applications

To achieve best performance for Kerberos SSO, we recommend SSH platforms based on OpenSSH 4.3 or higher. Sun Solaris SunSSH 1.2 also performs optimally.

For best performance, the AD Bridge **NssEnumerationEnabled** setting (**config --detail NssEnumerationEnabled**) should be set to **false**, which is not the default. Many applications make use of the **getent()** family of functions for PAM-based authentication (**getpwent()** and **getgrent()** in particular). For applications that claim PAM support but do not work with **NssEnumerationEnabled** set to **false**, **NssEnumerationEnabled** may need to be set to **true**.

Account Management

Best practices for managing service, application, and user accounts.

Service Accounts

Applications that run as a process on a host as a user ID should be run as a local service account. Users should not authenticate as these accounts, but instead use sudo or some similar process to authenticate as themselves with the authorization to run commands on behalf of the service account.

Application Accounts

Applications that authenticate to another host as a user ID should use an application account based in AD, and managed by the customer's SOP for application or service accounts in AD.

User Accounts

All accounts that can be mapped back to a single person should be based in AD and not exist locally. If there is no account for this person in AD, the account should be moved to AD.

Unix Best Practices Summary

- Any time SSH is upgraded, **domainjoin-cli configure --enable ssh** should be run.
- After any major system upgrade is performed, a full rejoin to the domain should be performed.

- Apply all vendor patches per the vendor schedule.
- Solaris 11.4 or higher is recommended.
- Install AD Bridge on Solaris Zones individually.
- SSH platforms based on OpenSSH 4.3 or higher is recommended.

AD Bridge Operations Best Practices

Before taking any actions with AD Bridge Operations, review these best practices carefully.

IMPORTANT!

*The Named Service Cache Daemon (NSCD) cache **must** be disabled as it conflicts with ADB.*

Uninstall SSSD and Centrify

AD Bridge is not compatible with **System Security Services Daemon (SSSD)** or **Centrify**. Uninstall SSSD and Centrify from any Linux computers where you want to deploy the AD Bridge agent.

SSH Logons

Because AD Bridge canonicalizes NT4-style and UPN-style log on names to the chosen display method (alias, short, or long name), users should be encouraged to use the same username on Windows and Unix systems. This provides log on name simplicity to the end user, and gives any troubleshooters a clear knowledge of the specific AD user in question, as well as the knowledge that the user is an AD user. Users will still be presented with their alias name once logged into the server.

Lookups and Configuration

Many Unix applications like sudo and chown will look up AD users through the AD Bridge-provided interfaces. In all cases where possible, best practices are to configure these applications to use the canonical (displayed or alias) name for all lookups, rather than the NT4-style or UPN-style names that AD Bridge understands.

Operating System Patching and Upgrades

When any Unix operating system is upgraded or patched, it is highly likely that AD Bridge-related files will be changed. For example, RPM-based Linux systems will overwrite PAM configuration for any package which uses PAM when that package is upgraded.

We recommend that the computer be fully rejoined to the domain after each OS upgrade. Minor patches which only affect PAM or NSSwitch configuration can be followed with the **domainjoin-cli configure** command. In all cases, all OS upgrades and patches should be tested for compatibility with the AD Bridge configuration changes prior to wide company adoption.

IMPORTANT!

*For any Unix operating system upgrade or patch, you must back up all PAM files to a different location (other than the PAM directory) to mitigate module errors on **domainjoin**, prior to the upgrade or patch being applied.*

Operations Best Practices Summary

- Uninstall **SSSD** and **Centrify** from Linux computers where you want to deploy the AD Bridge agent.
- The NSCD cache **must** be disabled.

- Encourage users to use the same username on Windows and Unix systems.
- Configure applications applications like sudo and chown to use the canonical (displayed or alias) name for all lookups.
- All OS upgrades and patches should be tested for compatibility with the AD Bridge configuration changes.
- After each OS upgrade, fully rejoining the computer to the domain is recommended.